07-1805

AF

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/574,345
Filing Date	May 19, 2000
First Named Inventor	Derek C. AU
Art Unit	2143
Examiner Name	K. H. Shin
Total Number of Pages in This Submission	
Attorney Docket Number	578062000300

ENCLOSURES (*Check all that apply*)

- [x] Fee Transmittal Form
- [ ] Fee Attached
- [ ] Amendment/Reply
- [ ] After Final
- [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
- [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Return Receipt Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

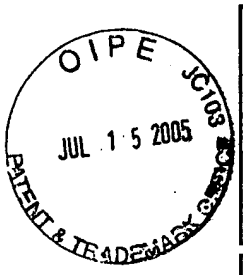
Firm Name	MORRISON & FOERSTER LLP (Customer No. 25224)		
Signature			
Printed name	David T. Yang		
Date	July 15, 2005	Reg. No.	44,415

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 506673936US, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: July 15, 2005 Signature: _____ (Marco Jimenez)

la-806058

PTO/SB/17 (12-04v2)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no person are required to respond to a collection of information unless it displays a valid OMB control number.



Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	09/574,345
Filing Date	May 19, 2000
First Named Inventor	Derek C. AU
Examiner Name	K. H. Shin
Art Unit	2143
Attorney Docket No.	578062000300

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 03-1952 Deposit Account Name: Morrison & Foerster LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 =	_____	x _____	= _____

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 =	_____	x _____	= _____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____	/50 _____ (round up to a whole number) x	_____	= _____

4. OTHER FEE(S) **Fees Paid ($)**

Non-English Specification, $130 fee (no small entity discount)

Other (e.g., late filing surcharge): 1402 Filing a brief in support of an appeal 500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	44,415	Telephone	(213) 892-5587
Name (Print/Type)	David T. Yang			Date	July 15, 2005

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV 506673936US, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: July 15, 2005 Signature: (Marco Jimenez)

Docket No.: 578062000300
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
AU et al.

Application No.: 09/574,345 Confirmation No.: 8281

Filed: May 19, 2000 Art Unit: 2143

For: CRYPTOGRAPHIC COMMUNICATIONS USING PSEUDO-RANDOMLY GENERATED CRYPTOGRAPHIC KEYS Examiner: Shin, Kyung H

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on June 3, 2005 and is in furtherance of said Notice of Appeal.

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I.	Real Party In Interest
II	Related Appeals and Interferences
III.	Status of Claims
IV.	Status of Amendments
V.	Summary of Claimed Subject Matter
VI.	Grounds of Rejection to be Reviewed on Appeal
VII.	Argument
VIII.	Claims Appendix
IX.	Evidence Appendix
X.	Related Proceedings Appendix
Appendix A	Claims

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is StealthKey, Inc., the current assignee of the above application.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Current Status of Claims

1. Claims canceled: 3, 17-22

2. Claims withdrawn from consideration but not canceled: none

3. Claims pending: 1, 2, and 4-16

4. Claims allowed: none

5. Claims rejected: 1, 2, and 4-16

B. Claims on Appeal

The claims on appeal are claims 1, 2, and 4-16, of which Claims 1, 10, and 15 are independent claims.

IV. STATUS OF AMENDMENTS

Applicant did not file any amendments in response to the rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to a secured cryptographic communications system in which the communication nodes of the system include a pseudo-random key generator for generating, locally and independently, pseudo-random keys that can be used to encrypt/decrypt communication data (see Figs. 2-5). Since the cryptographic keys can be generated locally at each of the communication nodes, the keys need not be transported between the communication nodes and hence the communication system is not susceptible to compromise via interception of keys. In accordance with a preferred embodiment of the present invention, a cryptographic key based on pseudo-randomly generated numbers are generated at all of the communication nodes within an authorized user community once every key change period, starting from a predetermined/stored reference initialization value (referred to as the crypto midnight date and time value in the specification).

In order to ensure that the pseudo-random key generators are using the same keys at the same time, the pseudo-random key generators should preferably be initiated at the same exact time and are preferably periodically synchronized with each other thereafter. However, in practice, it is impractical to initialize the different units of pseudo-random key generators at the exact same time, especially if the units are located in different parts of the world. Although it is possible for the manufacturer to initialize the units at the same time at the factory, subscribers of the system may not wish to have the generators activated at the factory for reasons of fearing comprising the generated keys during the transportation or shipping of the pseudo-random key generators. It is more secure to initialize the pseudo-random key generators after they have been delivered to their intended users.

One of the important advantages offered by the present invention is the ability to initialize the pseudo-random key generators at different times while ensuring that the pseudo-random key generators will generate the same pseudo-random keys at the same time. To accomplish this objective, an initialization unit is included in the pseudo-random key generators, wherein the initialization units (such as the time/key initialize device 108 shown in Fig. 1), upon activating the pseudo-random key generator, will check a current data and time against the crypto midnight initialization date and time (CMDT) and determine a difference between the two time values. Using the difference in timing values the initialization unit determines how many predetermined key change periods have passed since the initialization date and time, and cause the pseudo-random number generator of the pseudo-random key generator to cycle through the generations of pseudo-random numbers from the CMDT through the current time value, effectively synchronizing the pseudo-random key generator.

A. Summary of Claimed Subject Matter in Independent Claim 1

Claim 1 is directed to a pseudo-random key generator ("PKG") for use in a symmetrical-key cryptographic communication system. The PKG includes a timing circuit 114 and a pseudo-random number generator ("PRN") 105 that generate a numerical value (including alphanumeric values) periodically in accordance with predetermined key change periods. The PKG, upon initialization, performs a step of comparison to compare a current time value (such as a current date and the time of the day) against a crypto midnight value that was installed into the PKG at the factory (see Fig. 1). As described in the last paragraph of Page 12 of the present application, once a delta time is determined from the comparison step, the PRN generator cycles through the numerical

sequences for all the key change periods between the midnight value and the detected a current time to achieve synchronization.

B. Summary of Claimed Subject Matter in Independent Claims 10 and 15

Claim 10 and (method version thereof Claim 15) is directed to a cryptographic communication system (such as the ones illustrated in Figs. 2-5) that uses a PKG as described immediately above. Again, the PKG includes a timing circuit 114 and a pseudo-random number generator ("PRN") 105 that generate a numerical value (including alphanumeric values) periodically in accordance with predetermined key change periods. And again, the PKG, upon initialization, performs a step of comparison to compare a current time value (such as a current date and the time of the day) against a crypto midnight value that was installed into the PKG at the factory (see Fig. 1).

Claim 10 (and Claim 15) also recites computer storage areas for storing a lookup table (e.g., the PRN re-map table 109) and a key formation table (e.g., the key block formation table 110) for use in conjunction with the PRN generator 105 to generate crypto keys. The use of a lookup table and a key formation table enhances the security of the cryptographic system. Specifically, the use of the lookup table and the key formation table further scrambles the algorithm used for generating the pseudo random numbers.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, and 4-16 are rejected under 35 U.S.C. 103 as being unpatentable over Jones (U.S. patent No. 5,412,730) in view of Lynn (U.S. patent no. 5,345,508) and further in view of Dent (U.S. patent no. 5,060,266).

VII. ARGUMENT

For the reasons stated below, Applicants respectfully submit that none of the cited references contain any disclosure or suggestion of a pseudo-random key generator that can perform an initialization procedure to synchronize itself with a crypto midnight initialization value as recited in the claims.

First, Applicants note that Jones is directed to an encryption data system that is dependent upon "block counting" technique for generating cryptographic keys. The Examiner repeatedly acknowledged during the prosecution of the present application that Jones does not disclose generating cryptographic keys based on sequences of time or periods of time. Furthermore, Jones does not deal with the initialization of pseudo-random key generators to ensure that the different units can generate consistent keys while being activated at different times.

Applicants respectfully submit that neither Dent nor Lynn makes up for the deficiencies of Jones.

Specifically, Dent is directed to a system for synchronizing encryption devices and for the resynchronization of a sender and a receiver unit should the two devices fall out of synchronization; Dent does not teach or suggest an initialization procedure such that pseudo-random key generators may be activated at different times and still generate symmetrical keys for a given time value.

Lynn, on the other hand, discloses a system whereby pseudorandom cryptographic keys are generated by both a transmitter and a receiver. The stated purpose of Lynn is to conserve processing resources by saving generated cryptographic keys that correspond to a given initialization vector (see col. 2, lines 19-33). In particular, as discussed in column 2, lines 58 to column 3, line 5:

> "Both the transmitter and receiver share a common secret key that has been communicated through some separate channel. The transmitter combines the secret key (which serves as a constant base value) with an Initialization Vector (IV), using an XOR operation to produce a temporal key. This temporal key is then used as an input to a pseudorandom number (PN) generator to produce a unique PN sequence of binary digits, for each new temporal key entered. . . . The initialization vector together with its corresponding PN sequence is then stored in a cache and the PC sequence is iteratively reused, as determined by a counter, to encrypt one or more plaintext messages."

In other words, each time the transmitter sends a message, an initialization vector is first sent to the receiver, which will combine the received initialization vector with the common secret key via and XOR operation, the result of which is inputted into the PN generator for generating a sequence of binary numbers for decrypting the received message. The initialization vector, along with the corresponding generated PN sequence binary number, is at the same time stored in a memory for later use. In the event an initialization vector is re-used by the transmitter at a later time, the receiver will simply retrieve the previously generated sequence binary number rather than performing the XOR operation and inputting the XOR result into the PN generator again.

In summary, Lynn discloses utilizing a sequence generator at both ends of a communication channel wherein the sequence generators will generate an unique output for each unique input, wherein the input is a XOR product of a common secret key and an initialization vector that is transmitted from the transmitter to the receiver each time a message is to be sent. To

conserve processing resources, the initialization vectors are reused, and the generated sequence numbers are stored in a cache for later retrieval rather than re-generating the sequence number.

In contrast, the present invention does not require transmitting an initialization vector value to the receiver each time a message is to be sent. An important advantage of the present invention is that, once the pseudorandom cryptographic key generators are initialized, identical cryptographic keys are automatically generated at both the receiver and the transmitter without any need to provide any additional inputs or "initialization vectors." However, to compensate for different initialization times of different generators, upon initialization a generator first checks the current time against the crypto-midnight time (i.e., the preset initialization time), and brings the generator to synchronization with the transmitter generator. For instance, if the crypto-midnight value is 12:00 a.m., and the current time upon initialization is 3:00 a.m., and if the predetermined key change period is 10 minutes, then the initialized generator will "fast forward" the generation of sequence numbers by 18 key change periods to bring the generator to synchronization with the system.

Applicants respectfully submit that the above-described aspects of the invention as claimed are simply not disclosed by any of the references cited.

The Examiner in the final Office Action points to column 2, lines 48-53 of Lynn as teaching this feature of the present invention. However, that section of Lynn simply states: "It is therefore desirable that a high speed cryptosystem exhibit the property of self-synchronization between transmitter and receiver such that no additional recovery procedures are required to decode messages." As one can surely appreciate, this is nothing more than stating a general goal; it does

not teach nor suggest the details of the present invention as claimed whatsoever. There is simply no teaching, by any of the references, of the initialization step as recited in all of the claims.

With further respect to Claim 10 and 15, the use of the lookup and key tables (stored in computer memory) provides the advantage of lowering the required processing power for generating more complex or lengthier pseudo random numbers. In particular, a basic pseudo random number generation cryptographic system may be prone to attack if an attacker has access to the pseudo randomly generated numbers (e.g., a pseudo random cryptographic system using portable user key fobs typically displays the pseudo randomly generated numbers) and can use a sequence of the pseudo randomly generated numbers to derive the algorithm used for generating the pseudo random numbers. In order to build a robust pseudo random cryptographic system, it is preferable to use a complex algorithm and/or generate pseudo random numbers both very high orders. However, in practice, communication nodes for the consumer market (such as a key fob or a smart card) may not have enough processing power to execute such complex algorithms or generate high order pseudo random numbers. Accordingly, the use of lookup tables and key block formation tables, the stored values of which may have no numerical relationships to each other, allows one to build a robust pseudo random cryptographic communication system without having to use very complex algorithms or require the generation of high order pseudo random numbers. An attacker who records a sequence of the table values would find it impossible to derive the algorithm since the values have no numerical relationships to each other.

Applicants respectfully submit that such features and advantages are not disclosed or suggested by any of the references. Jones, the primary reference relied upon by the Examiner as

disclosing this aspect of the invention, simply discloses a key memory 50 for storing a current encryption value); no mention whatsoever is made of a lookup table for retrieving values (via the pseudo randomly generated number) to be used to retrieve a key value.

In view of the above, Applicant respectfully appeals from the Examiner's rejection in the Final Office Action.

VIII. CLAIMS APPENDIX

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Examiner is being submitted.

X. RELATED PROCEEDINGS APPENDIX

No related proceedings are referenced above, hence no Appendix is included.

Dated: July 15, 2005

Respectfully submitted,

By _____
David T. Yang
Registration No.: 45,415
MORRISON & FOERSTER LLP
555 West Fifth Street
Los Angeles, California 90013-1024
(213) 892-5587

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/574,345

Claim 1 A pseudo-random key generator for use within a cryptographic communication system, said pseudo-random key generator comprising:

a pseudo-random number generator for periodically generating a plurality of pseudo-random numbers, wherein a pseudo-random number is generated for every occurrence of a predetermined key change period;

a computer readable storage medium connected to said pseudo-random number generator;

a timing circuit operatively coupled to said pseudo-random number generator, said timing circuit includes a time/key initialization device and a timing source for providing current timing values,

wherein, upon initialization of the pseudo-random key generator, said timing source compares a current timing value with a predetermined crypto midnight initialization timing value, and transmits the difference to the time/key initialization device, which causes the pseudo-random number generator to generate a set of initialization pseudo-random numbers starting from the crypto midnight initialization timing value until a pseudo-random number is generated in sequence for all of the key change periods between the crypto midnight initialization timing value and the current timing value.

Claim 2 The pseudo-random key generator according to claim 1, wherein said timing circuit further includes a delta counter operatively coupled to said time/key initialization device.

Claim 3 (canceled)

Claim 4 The pseudo-random key generator according to claim 1, wherein said computer readable storage medium includes a PRN re-map table.

Claim 5 The pseudo-random key generator according to claim 1, wherein said computer readable storage medium includes a PRN re-map table.

Claim 6 The pseudo-random key generator according to claim 1, further comprising a read only computer readable storage medium connected to said timing circuit.

Claim 7 The pseudo-random key generator according to claim 6, wherein said read only computer readable storage medium includes:

the crypto midnight initialization timing value; and

the key change period value.

Claim 8 The pseudo-random key generator according to claim 6, wherein said computer readable storage medium includes an executable program, said executable program causing said systems re-map generator to re-map the data of said PRN re-map table.

Claim 9 The pseudo-random key generator according to claim 8, wherein said system re-map generator selectively rearranges data stored in said computer readable storage medium.

Claim 10 A cryptographic communication system having a pseudo-random key generator for generating cryptographic keys, said pseudo-random key generator comprising:

a pseudo-random number generator;

a timing circuit operatively coupled to said pseudo-random number generator, said timing circuit providing a sequence of current timing values;

a first computer readable storage area operatively coupled to said pseudo-random number generator, said first computer readable storage area containing a plurality of data values, each data value associated with a unique storage address within said first computer readable storage area;

a second computer readable storage area operatively coupled to said first computer readable storage area, said second computer readable storage area containing a plurality of key data values, each key data value associated with a unique storage address within said second computer readable storage area,

wherein the pseudo-random number generator periodically generates a pseudo-random number for every predetermined key change period, wherein each generated pseudo-random number is used to look up a unique address in the first computer readable storage area for retrieving the data value associated with the looked up unique address, and wherein the retrieved data value is used to look up a unique address in the second computer readable storage area for retrieving a key value data, said key value data being used to form a cryptographic key,

wherein, upon initialization of the pseudo-random key generator, said timing circuit compares a current timing value with a predetermined crypto midnight initialization timing value and cause the pseudo-random number generator to generate a set of initialization pseudo-random numbers starting from the crypto midnight initialization timing value until a pseudo-random number

is generated for all of the key change periods between the crypto midnight initialization timing value and the current timing value.

Claim 11 The cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said first computer readable storage area for generating the data values in accordance with a predetermined algorithm.

Claim 12 The cryptographic communication system according to claim 11, wherein said programmed processor selectively rearranges the data values in said first computer readable storage area.

Claim 13 The cryptographic communication system according to claim 10, further comprising a programmed processor operatively coupled to said second computer readable storage area for generating the key data values in accordance with a predetermined algorithm.

Claim 14 The cryptographic communication system according to claim 13, wherein said programmed processor selectively rearranges the key data values in said second readable storage area.

Claim 15 A method of generating cryptographic keys using a pseudo-random number generator, a first computer readable storage area, and a second computer readable storage area, said method comprising the steps of:

inputting into said pseudo-random number generator an initial data value;

initializing said pseudo-random number generator, said step of initialization includes steps of determining a difference between a crypto midnight initialization time value and a current time value, and causing said pseudo-random number generator to generate a set of initial pseudo-random numerical values;

generating a current time pseudo-random numerical value;

generating a first data string by using said generated current time pseudo-random numerical value to look up a unique memory address in the first computer readable storage area and retrieving a data value associated with the unique memory address in the first compute readable storage area, said data value being one of a plurality of data values stored in the first computer readable storage area; and

generating a second data string by using said first data string to look up a unique memory address in the second computer readable storage area and retrieving a key data value associated with the unique memory address in the second compute readable storage area, said key data value being one of a plurality of key data values stored in the second computer readable storage area,

wherein the retrieved key data value is used to form a cryptographic key.

Claim 16 The method according to claim 15, further comprising the steps of:

rearranging the order of the plurality of data values stored in the first computer readable storage area; and

rearranging the order of the plurality of key data values stored in the second computer readable storage area

Claims 17-22 (canceled)